ARMONÍA DENTO-FACIAL

Cirugía Maxilofacial · Implantología Cortical Avanzada

SISTEMA INTEGRAL DE

PROTECCIÓN DE DATOS PERSONALES, POLÍTICA DE PRIVACIDAD Y ACUERDOS DE CONFIDENCIALIDAD

Conforme a la Ley 1581 de 2012, Decreto 1377 de 2013,
Reglamento General de Protección de Datos (RGPD — UE 2016/679)
y Health Insurance Portability and Accountability Act (HIPAA — EE.UU.)

Versión 1.0 · Vigente desde abril de 2026

RESUMEN EJECUTIVO

El presente documento constituye el marco integral de protección de datos personales, privacidad, seguridad de la información y confidencialidad adoptado por la Clínica Armonía Dento-Facial (en adelante, "la Clínica" o "el Responsable"), con el propósito de garantizar a sus pacientes —nacionales e internacionales—, colaboradores y terceros, que todo tratamiento de información se realiza bajo los más altos estándares jurídicos, éticos y técnicos aplicables al sector salud.

La Clínica, en su condición de prestador de servicios especializados en cirugía maxilofacial e implantología cortical, gestiona información de naturaleza particularmente sensible: historias clínicas, imágenes diagnósticas de alta resolución (radiografías panorámicas, tomografías computarizadas de haz cónico —CBCT—, fotografías clínicas), condiciones preexistentes y resultados de procedimientos quirúrgicos. Consciente de la delicadeza de estos datos, adopta un régimen de cumplimiento multinivel fundamentado en:

- Ley Estatutaria 1581 de 2012, Decreto Reglamentario 1377 de 2013 y Circulares de la Superintendencia de Industria y Comercio (SIC) de Colombia.
- Reglamento (UE) 2016/679 — Reglamento General de Protección de Datos (RGPD), aplicable a pacientes residentes en el Espacio Económico Europeo.
- Health Insurance Portability and Accountability Act (HIPAA) y su Privacy Rule, como referente para pacientes estadounidenses.
- Resolución 1995 de 1999 y Resolución 839 de 2017 del Ministerio de Salud y Protección Social de Colombia, en materia de historia clínica.
- Resolución 2654 de 2019 sobre telesalud y normas concordantes.

> **Compromiso institucional**
>
> *La Clínica Armonía Dento-Facial concibe la protección de los datos personales no como una obligación administrativa, sino como una extensión natural del deber de cuidado médico. La confidencialidad que rige la relación médico-paciente se traslada íntegramente al plano digital, con las garantías técnicas, organizativas y jurídicas que hoy exige el Estado del Arte.*

Este documento se estructura en once (11) Títulos, cuarenta y tres (43) artículos y cinco (5) anexos normativos, abordando de manera sistemática la identificación de datos, las finalidades autorizadas, los derechos del titular, la seguridad de la información, la transferencia internacional, la política de cookies, el consentimiento informado para telemedicina y los modelos contractuales de confidencialidad aplicables al personal y terceros.

TÍTULO I — DISPOSICIONES GENERALES

Artículo 1. Identificación del Responsable del Tratamiento

El Responsable del Tratamiento de los Datos Personales es la CLÍNICA ARMONÍA DENTO-FACIAL, persona jurídica constituida conforme a las leyes de la República de Colombia, con los siguientes datos de contacto:

a) Denominación social: Armonía Dento-Facial S.A.S. (o la razón social que corresponda).

b) NIT: [Número de Identificación Tributaria].

c) Domicilio principal: [Dirección física completa], Colombia.

d) Correo electrónico de contacto para asuntos de privacidad: protecciondedatos@armoniadentofacial.co

e) Teléfono: [Indicativo +57] [Número].

f) Sitio web oficial: www.armoniadentofacial.co

g) Oficial de Protección de Datos (DPO): [Nombre completo], correo electrónico: dpo@armoniadentofacial.co

Artículo 2. Objeto y Ámbito de Aplicación

La presente política tiene por objeto establecer los lineamientos, principios, finalidades, procedimientos y mecanismos que observará la Clínica para la recolección, almacenamiento, uso, circulación, supresión, transferencia y transmisión de datos personales de sus pacientes, acompañantes, representantes legales, colaboradores, proveedores, aliados estratégicos y cualquier otro titular cuya información sea tratada en el marco de sus operaciones.

El presente documento aplica a todos los procesos, sistemas de información, plataformas digitales, canales de atención, bases de datos físicas o electrónicas administradas por la Clínica o por terceros encargados del tratamiento en virtud de contrato vigente.

Artículo 3. Marco Normativo Aplicable

La Clínica adopta un modelo de cumplimiento normativo multinivel, en reconocimiento de la naturaleza transfronteriza de sus servicios clínicos. Son fuentes obligatorias del presente sistema:

3.1 Normativa nacional colombiana

- Constitución Política de Colombia, artículo 15 (habeas data).
- Ley 1581 de 2012, "por la cual se dictan disposiciones generales para la protección de datos personales".
- Decreto 1377 de 2013, reglamentario parcial de la Ley 1581 de 2012.
- Decreto 1074 de 2015 (Decreto Único Reglamentario del Sector Comercio).

- Ley 1266 de 2008 (Habeas Data Financiero), cuando aplique.
- Resolución 1995 de 1999 del Ministerio de Salud (historia clínica).
- Ley 23 de 1981 (Código de Ética Médica) y Ley 35 de 1989 (Código de Ética del Odontólogo).
- Resolución 2654 de 2019 del Ministerio de Salud (telesalud y telemedicina).
- Circulares 002 y 003 de 2015 de la Superintendencia de Industria y Comercio.

3.2 Normativa internacional de referencia

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo — RGPD.
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) y HITECH Act.
- Convenio 108+ del Consejo de Europa para la protección de datos personales.
- Estándar ISO/IEC 27001 (Sistema de Gestión de Seguridad de la Información).
- Estándar ISO/IEC 27799 (Gestión de Seguridad de la Información en Salud).

Artículo 4. Definiciones

Para efectos de la correcta interpretación del presente documento, se adoptan las siguientes definiciones, armonizadas con el artículo 3 de la Ley 1581 de 2012 y el artículo 4 del RGPD:

a) Autorización: consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de sus datos personales.

b) Base de Datos: conjunto organizado de datos personales objeto de tratamiento.

c) Dato Personal: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

d) Dato Sensible: aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar discriminación; incluyen, sin limitarse a, datos de salud, historia clínica, datos biométricos, imágenes diagnósticas, origen racial, ideología política, convicciones religiosas, vida sexual, entre otros.

e) Encargado del Tratamiento: persona natural o jurídica que realiza el tratamiento por cuenta del Responsable.

f) Responsable del Tratamiento: la Clínica Armonía Dento-Facial, quien decide sobre la base de datos y el tratamiento.

g) Titular: persona natural cuyos datos son objeto de tratamiento (paciente, acompañante, colaborador, etc.).

h) Tratamiento: cualquier operación sobre datos personales: recolección, almacenamiento, uso, circulación, supresión, transmisión o transferencia.

i) Transferencia Internacional: envío de datos a un Responsable ubicado fuera del territorio colombiano.

j) Transmisión: comunicación de datos a un Encargado para que los trate por cuenta del Responsable.

k) Telemedicina: prestación de servicios de salud mediada por tecnologías de la información y la comunicación, conforme a la Resolución 2654 de 2019.

l) Historia Clínica Electrónica (HCE): documento privado, obligatorio y sometido a reserva, que registra cronológicamente las condiciones de salud del paciente.

Artículo 5. Principios Rectores

El tratamiento de datos personales se rige por los siguientes principios:

a) Legalidad: actividad reglada, sujeta a la Ley 1581 y normas concordantes.

b) Finalidad: las finalidades serán legítimas, informadas al Titular y conforme con la Constitución.

c) Libertad: el tratamiento requiere consentimiento previo, expreso e informado.

d) Veracidad o calidad: la información será veraz, completa, exacta, actualizada, comprobable y comprensible.

e) Transparencia: se garantiza el derecho del Titular a obtener información sobre sus datos.

f) Acceso y circulación restringida: el tratamiento solo podrá hacerse por personas autorizadas.

g) Seguridad: medidas técnicas, humanas y administrativas necesarias para evitar adulteración, pérdida, consulta, uso o acceso no autorizado.

h) Confidencialidad: todas las personas que intervienen están obligadas a garantizar la reserva de la información.

i) Minimización (RGPD, Art. 5.1.c): tratamiento limitado a lo necesario para las finalidades.

j) Responsabilidad proactiva (accountability): la Clínica demostrará cumplimiento mediante documentación y auditorías.

TÍTULO II — IDENTIFICACIÓN Y CATEGORIZACIÓN DE LOS DATOS TRATADOS

Artículo 6. Datos Personales de Identificación y Contacto

La Clínica recolecta, para finalidades administrativas, relacionales y de identificación inequívoca del paciente, los siguientes datos de categoría general:

- Nombres y apellidos completos.
- Tipo y número de documento de identidad (cédula de ciudadanía, cédula de extranjería, pasaporte).
- Fecha y lugar de nacimiento.
- Nacionalidad y país de residencia.
- Dirección de residencia o correspondencia.
- Número(s) de teléfono fijo y móvil.
- Dirección de correo electrónico.
- Ocupación o actividad económica.
- Entidad Promotora de Salud (EPS) o seguro médico internacional, cuando aplique.
- Nombre y datos de contacto de persona responsable o de emergencia.

Artículo 7. Datos Sensibles — Información Clínica y de Salud

En estricto cumplimiento del artículo 6 de la Ley 1581 de 2012 y del artículo 9 del RGPD, la Clínica declara que trata datos sensibles de naturaleza clínica, los cuales están sujetos a un régimen reforzado de protección, consentimiento explícito y confidencialidad absoluta. Estos incluyen:

- Historia clínica electrónica completa (anamnesis, evolución, planes terapéuticos).
- Condiciones de salud preexistentes (diabetes, hipertensión, coagulopatías, alergias, enfermedades sistémicas).
- Antecedentes médicos, quirúrgicos y farmacológicos.
- Resultados de exámenes clínicos, paraclínicos y de laboratorio.
- Diagnósticos, planes de tratamiento y prescripciones.
- Información sobre consumo de sustancias (tabaco, alcohol, medicamentos).
- Datos genéticos o biométricos, en caso de ser recolectados.
- Información sobre estado de salud mental relacionada con el tratamiento odontomaxilofacial.

Artículo 8. Imágenes Diagnósticas y Documentación Visual

> **Régimen especial de imágenes clínicas**
>
> *Las imágenes diagnósticas, por su capacidad de identificar unívocamente al paciente, su naturaleza biométrica y su valor pericial, reciben un nivel de protección equivalente al más alto estándar aplicable a datos de categoría especial conforme al artículo 9 del RGPD.*

Se catalogan bajo este régimen:

- Radiografías periapicales, panorámicas y cefalométricas.
- Tomografías computarizadas de haz cónico (CBCT) y volúmenes DICOM.
- Fotografías intraorales y extraorales (frontales, laterales, sonrisa, perfil).
- Escaneos intraorales 3D y modelos digitales (archivos STL, PLY, OBJ).
- Registros videográficos quirúrgicos o de consulta.
- Imágenes de resonancia magnética (MRI), si aplican al caso.

Toda imagen diagnóstica se almacena cifrada, con metadatos disociados cuando sea posible, y su acceso queda restringido al personal clínico tratante mediante controles de identidad y registro de auditoría (logs).

Artículo 9. Datos de Menores de Edad

Conforme al artículo 7 de la Ley 1581 de 2012, el artículo 12 del Decreto 1377 de 2013 y el artículo 8 del RGPD, el tratamiento de datos personales de menores de edad requiere la autorización previa, expresa e informada del representante legal. La Clínica:

1. Recolectará únicamente los datos estrictamente necesarios para la prestación del servicio de salud al menor.
2. Respetará el interés superior del menor y los derechos fundamentales que le asisten.
3. Escuchará la opinión del menor, valorada en relación con su madurez, autonomía y capacidad para entender el asunto.
4. Mantendrá los datos bajo el mismo régimen reforzado aplicable a datos sensibles.

Artículo 10. Datos Financieros y de Facturación

Para efectos de facturación, cobranza, pago electrónico y cumplimiento de obligaciones tributarias, la Clínica podrá recolectar:

- Información de medios de pago (enmascarada según estándar PCI-DSS; la Clínica no almacena números completos de tarjetas).
- Comprobantes de pago, constancias bancarias y referencias de transferencia.
- Información de facturación: nombre o razón social, NIT/documento, dirección fiscal.

- Historial de pagos y saldos pendientes.

Tabla resumen de categorías de datos

Categoría	Ejemplos	Nivel de protección
Datos de identificación	Nombre, documento, fecha de nacimiento	Estándar
Datos de contacto	Correo, teléfono, dirección	Estándar
Datos sensibles — Salud	Historia clínica, alergias, diagnósticos	Reforzado
Imágenes diagnósticas	Radiografías, CBCT, fotografías clínicas	Reforzado (biométrico)
Datos de menores	Cualquiera de las anteriores en <18 años	Reforzado + consentimiento tutor
Datos financieros	Facturación, medios de pago enmascarados	Estándar + PCI-DSS

TÍTULO III — FINALIDADES DEL TRATAMIENTO

Los datos personales son tratados única y exclusivamente para las finalidades informadas al Titular al momento de recolectar su autorización. Cualquier finalidad ulterior requerirá un nuevo consentimiento.

Artículo 11. Finalidades Administrativas y Relacionales

a) Identificación inequívoca del paciente y gestión de su expediente.

b) Programación, confirmación, recordatorio y reprogramación de citas clínicas.

c) Comunicación relacionada con el tratamiento, indicaciones pre y postoperatorias, controles.

d) Atención de consultas, peticiones, quejas y reclamos (PQRS).

e) Envío de información administrativa (cambios de horario, cierres, novedades operativas).

f) Facturación, cobranza, contabilidad y cumplimiento de obligaciones tributarias.

g) Gestión de autorizaciones ante entidades aseguradoras o planes de beneficios.

Artículo 12. Finalidades Asistenciales, Clínicas y Diagnósticas

a) Elaboración, conservación y actualización de la historia clínica conforme a la Resolución 1995 de 1999.

b) Realización de estudios diagnósticos: radiografías, tomografías, escaneos intraorales, fotografías.

c) Análisis y planificación de tratamientos quirúrgicos maxilofaciales e implantológicos.

d) Diseño digital de sonrisa, guías quirúrgicas, modelos protésicos y prótesis dentales.

e) Coordinación con laboratorios dentales, protésicos, centros de imagenología y aliados clínicos.

f) Seguimiento postoperatorio y controles evolutivos.

g) Interconsulta entre especialistas tratantes.

h) Atención de urgencias y complicaciones clínicas.

i) Respuesta a requerimientos judiciales, administrativos o sanitarios legalmente soportados.

Artículo 13. Finalidades de Marketing, Comunicación y Casos de Estudio

> **Consentimiento reforzado requerido**
>
> *Ningún dato personal —y en particular ninguna imagen clínica, fotografía o testimonio— será utilizado con fines promocionales, publicitarios, educativos o académicos sin la autorización expresa, específica, informada y libremente otorgada del Titular, mediante documento independiente a la autorización general de tratamiento de datos.*

Previo consentimiento explícito y separado, la Clínica podrá, como finalidades accesorias:

a) Publicar casos clínicos "antes/después" en el sitio web, redes sociales o material impreso.

b) Utilizar testimonios, videos o reseñas del paciente en campañas de comunicación.

c) Incluir imágenes anonimizadas en publicaciones científicas, ponencias académicas o cursos de formación.

d) Remitir boletines informativos, promociones, contenidos educativos y novedades de la Clínica.

e) Invitar a eventos, talleres o jornadas de salud bucal.

En todo caso, el paciente podrá revocar este consentimiento en cualquier momento, sin afectación alguna a la prestación del servicio de salud.

Artículo 14. Finalidades Legales, Regulatorias y de Calidad

a) Cumplimiento de obligaciones legales ante entes de control (Superintendencia Nacional de Salud, SIC, DIAN, Ministerio de Salud).

b) Habilitación y reacreditación de servicios de salud.

c) Auditorías internas y externas de calidad asistencial.

d) Farmacovigilancia, tecnovigilancia y reporte de eventos adversos.

e) Estudios estadísticos y epidemiológicos con datos disociados o anonimizados.

f) Defensa en procesos judiciales, disciplinarios o administrativos.

TÍTULO IV — AUTORIZACIÓN Y CONSENTIMIENTO

Artículo 15. Requisitos Generales de la Autorización

De conformidad con el artículo 9 de la Ley 1581 de 2012 y el artículo 4 del Decreto 1377 de 2013, la autorización del Titular debe ser:

a) Previa: obtenida antes del inicio del tratamiento.

b) Expresa: manifestada mediante acción afirmativa (firma, clic, audio, video).

c) Informada: precedida de información clara sobre responsable, finalidades, derechos y medios de contacto.

d) Libre: otorgada sin coacción, error, dolo, violencia o condicionamiento indebido.

e) Específica: individualizada para cada finalidad, cuando se trate de datos sensibles o finalidades secundarias.

La autorización puede obtenerse por medio físico (formulario firmado), electrónico (plataforma con doble confirmación) o cualquier otro que permita su posterior consulta y trazabilidad.

Artículo 16. Consentimiento Reforzado para Datos Sensibles

Tratándose de datos sensibles (salud, imágenes diagnósticas, biométricos), la Clínica obtendrá una autorización específica, adicional y separada de la autorización general, conforme al artículo 6 de la Ley 1581 de 2012. El Titular podrá negarse a entregar estos datos sin que ello signifique una violación de sus derechos; sin embargo, la negativa podrá impedir la prestación del servicio clínico solicitado, circunstancia que le será informada con claridad.

Artículo 17. Autorización para Menores de Edad

La autorización será otorgada por el padre, madre o representante legal del menor, quien firmará el documento correspondiente anexando copia de su identificación y del registro civil o documento que acredite la representación. En el caso de adolescentes, la Clínica procurará escuchar su opinión informada, valorada conforme a su grado de madurez.

Artículo 18. Revocatoria de la Autorización

El Titular podrá revocar en cualquier momento la autorización otorgada, total o parcialmente, mediante solicitud escrita dirigida a la Clínica. La revocatoria no tendrá efectos retroactivos sobre tratamientos anteriores legítimos, ni eximirá a la Clínica de conservar la información cuando exista obligación legal o contractual que lo imponga (por ejemplo, el deber de conservar la historia clínica durante los plazos previstos en la Resolución 839 de 2017).

TÍTULO V — DERECHOS DEL TITULAR

Artículo 19. Derechos ARCO — Ley 1581 de 2012

El Titular, conforme al artículo 8 de la Ley 1581 de 2012, tiene los siguientes derechos fundamentales frente al tratamiento de sus datos personales:

A) ACCESO: conocer, de manera gratuita y en cualquier momento, sus datos personales tratados por la Clínica, así como las finalidades, condiciones y destinatarios del tratamiento.

R) RECTIFICACIÓN: solicitar la corrección, actualización o complementación de datos parciales, inexactos, incompletos, fraccionados o que induzcan a error.

C) CANCELACIÓN (o supresión): requerir la eliminación de datos cuando su tratamiento no obedezca a los principios, derechos y garantías constitucionales y legales, o haya cesado la finalidad, salvo obligación legal de conservación.

O) OPOSICIÓN: negarse al tratamiento de sus datos cuando no exista obligación legal o contractual que lo imponga.

Artículo 20. Derechos Ampliados conforme al RGPD

Para los pacientes residentes en la Unión Europea o cuyo tratamiento esté sujeto al RGPD, la Clínica reconoce adicionalmente los siguientes derechos:

a) Derecho al olvido (Art. 17 RGPD): supresión de datos sin dilación indebida cuando concurran las causales legales, respetando los plazos de conservación clínica obligatorios.

b) Derecho a la portabilidad (Art. 20 RGPD): recibir los datos en formato estructurado, de uso común y lectura mecánica (JSON, XML, DICOM para imágenes), y transmitirlos a otro responsable.

c) Derecho a la limitación del tratamiento (Art. 18 RGPD): solicitar que el tratamiento se restrinja mientras se verifica la exactitud de los datos o se resuelve una oposición.

d) Derecho a no ser objeto de decisiones automatizadas (Art. 22 RGPD), incluida la elaboración de perfiles, que produzcan efectos jurídicos significativos sobre el Titular.

e) Derecho a presentar reclamación ante la autoridad de control competente (en Colombia, la SIC; en la UE, la autoridad nacional correspondiente).

Artículo 21. Procedimiento para el Ejercicio de Derechos

El Titular, sus causahabientes o representantes legales podrán ejercer sus derechos mediante los siguientes canales:

- Correo electrónico: protecciondedatos@armoniadentofacial.co
- Formulario electrónico disponible en www.armoniadentofacial.co/privacidad
- Comunicación escrita radicada en la sede principal de la Clínica.

- Atención presencial previa cita en el Departamento de Servicio al Paciente.

La solicitud deberá contener, como mínimo:

5. Identificación plena del Titular (copia del documento de identidad).
6. Descripción clara y precisa de los datos objeto de la solicitud y del derecho que se ejerce.
7. Dirección física o electrónica para notificaciones.
8. Documentos que soporten la solicitud, cuando aplique.
9. Firma autógrafa o electrónica del solicitante.

Artículo 22. Plazos de Respuesta

Tipo de solicitud	Plazo legal (Colombia)	Plazo RGPD
Consulta de datos	Diez (10) días hábiles	Un (1) mes
Reclamo / ARCO	Quince (15) días hábiles	Un (1) mes, prorrogable a tres
Notificación de brecha	Según instrucción SIC	Setenta y dos (72) horas
Revocatoria consentimiento	Inmediata	Inmediata

Cuando no fuere posible atender la consulta o el reclamo dentro de los plazos señalados, se informará al interesado los motivos de la demora y la fecha en que se atenderá, la cual en ningún caso superará los cinco (5) días hábiles siguientes al vencimiento del plazo inicial, conforme al artículo 14 de la Ley 1581 de 2012.

TÍTULO VI — TRANSFERENCIA Y TRANSMISIÓN INTERNACIONAL DE DATOS

Artículo 23. Pacientes Extranjeros y Flujo Transfronterizo

La Clínica, por su vocación internacional, atiende a pacientes residentes en países distintos a Colombia. En consecuencia, puede requerir transferir o transmitir datos personales a países extranjeros por motivos asistenciales (continuidad de la atención en el país de origen del paciente), administrativos (reembolsos de aseguradoras internacionales) o logísticos (coordinación de viajes médicos).

Artículo 24. Cláusulas Contractuales y Garantías

Toda transferencia internacional se efectuará bajo alguno de los siguientes instrumentos jurídicos, conforme al artículo 26 de la Ley 1581 de 2012 y los artículos 44 a 49 del RGPD:

a) Cláusulas contractuales tipo aprobadas por la Comisión Europea (Standard Contractual Clauses — SCC).

b) Declaración de conformidad expedida por la Superintendencia de Industria y Comercio, cuando se requiera.

c) Autorización expresa e informada del Titular para la transferencia específica.

d) Existencia de decisión de adecuación emitida por la autoridad competente.

e) Normas corporativas vinculantes (Binding Corporate Rules), cuando aplique a grupos internacionales.

Artículo 25. Países con Nivel Adecuado de Protección

Se considerarán países con nivel adecuado de protección aquellos reconocidos como tales por la Superintendencia de Industria y Comercio de Colombia (Circular Externa 005 de 2017) o por la Comisión Europea, incluyendo, entre otros: los Estados miembros de la Unión Europea, Argentina, Canadá, Uruguay, Nueva Zelanda, Japón, Suiza y Reino Unido, entre los actualizados por las autoridades competentes.

Cuando la transferencia se dirija a un país sin nivel adecuado, la Clínica adoptará garantías adicionales: cifrado extremo a extremo, seudonimización de datos identificables, limitación funcional y consentimiento específico del Titular.

TÍTULO VII — SEGURIDAD DE LA INFORMACIÓN

Artículo 26. Medidas Técnicas de Seguridad

En estricto cumplimiento del principio de seguridad (Art. 4.g Ley 1581) y del artículo 32 del RGPD, la Clínica ha implementado las siguientes medidas técnicas de protección:

26.1 Cifrado y criptografía

- Cifrado en tránsito: TLS 1.3 con suites criptográficas modernas (ECDHE/AES-GCM) para toda comunicación entre el navegador del paciente, el portal clínico y los servidores de la Clínica.
- Cifrado en reposo: AES-256 para bases de datos, sistemas de gestión clínica, repositorios de imágenes DICOM y respaldos (backups).
- Cifrado de dispositivos: BitLocker / FileVault en estaciones de trabajo clínicas; MDM con cifrado obligatorio en dispositivos móviles institucionales.
- Gestión de llaves: almacenamiento en Hardware Security Modules (HSM) o servicios de gestión de claves (KMS) certificados.

26.2 Control de acceso e identidad

- Autenticación multifactor (MFA) obligatoria para todo acceso a sistemas clínicos y administrativos.
- Principio de mínimo privilegio: cada colaborador accede únicamente a la información estrictamente necesaria para su función.
- Registro de auditoría (audit logs) inmutable, con retención mínima de dos (2) años, sobre toda consulta, modificación o exportación de datos clínicos.
- Revisión trimestral de accesos y revocación inmediata al término de la relación laboral.

26.3 Infraestructura y resiliencia

- Servidores en nube en centros de datos con certificación ISO/IEC 27001, SOC 2 Tipo II y cláusulas BAA cuando aplique a HIPAA.
- Redundancia geográfica y respaldos cifrados con periodicidad diaria incremental y semanal completa.
- Plan de continuidad del negocio (BCP) y recuperación ante desastres (DRP) con pruebas semestrales.
- Cortafuegos perimetral, WAF, segmentación de red y monitoreo 24/7 por centro de operaciones de seguridad.

Artículo 27. Medidas Organizativas

- Designación de un Oficial de Protección de Datos (DPO).

- Capacitación anual obligatoria del personal en protección de datos, confidencialidad y seguridad de la información.
- Evaluaciones de impacto en protección de datos (EIPD/DPIA) antes de introducir nuevos tratamientos de alto riesgo.
- Políticas internas de escritorio limpio, uso de dispositivos y teletrabajo.
- Gestión de proveedores con cláusulas obligatorias de protección de datos y auditoría.

Artículo 28. Gestión y Notificación de Incidentes de Seguridad

Ante la ocurrencia, sospecha o detección de un incidente de seguridad que comprometa datos personales, la Clínica activará el protocolo de respuesta a incidentes, que contempla:

10. Contención inmediata del incidente y preservación de evidencia digital.
11. Evaluación del alcance, naturaleza y severidad.
12. Notificación a la Superintendencia de Industria y Comercio conforme a la Circular 002 de 2015.
13. Notificación a los Titulares afectados sin dilación indebida, cuando el incidente suponga riesgo alto para sus derechos y libertades.
14. Notificación a la autoridad de control europea en un plazo no superior a 72 horas, si el RGPD resulta aplicable.
15. Análisis de causa raíz y adopción de medidas correctivas documentadas.

Artículo 29. Conservación y Supresión de Datos

La Clínica conservará los datos personales durante los plazos que exijan la ley y las buenas prácticas clínicas:

Categoría	Periodo de conservación	Fundamento
Historia clínica	Mínimo 15 años desde último contacto	Res. 839 de 2017 MSPS
Imágenes diagnósticas	Mínimo 15 años	Res. 1995/1999 y 839/2017
Datos de facturación	10 años	Estatuto Tributario y Código de Comercio
Datos de marketing	Hasta revocatoria del consentimiento	Ley 1581 de 2012
Registros de acceso (logs)	2 años mínimo	Estándar ISO 27001

Una vez vencidos los plazos, los datos serán suprimidos o anonimizados de manera irreversible mediante procedimientos certificados de destrucción de información.

TÍTULO VIII — ACUERDOS DE CONFIDENCIALIDAD

Artículo 30. Confidencialidad del Personal Interno

Todo colaborador de la Clínica —profesionales de la salud, personal administrativo, auxiliares, practicantes, contratistas y aprendices— suscribirá, como condición esencial de su vinculación, un Acuerdo de Confidencialidad y Deber de Reserva Clínica (Anexo B), cuyas obligaciones mínimas son:

a) Guardar reserva absoluta sobre cualquier información clínica, administrativa, financiera o comercial a la que tenga acceso, incluso después de terminada la relación laboral o contractual.

b) Abstenerse de divulgar, comentar, fotografiar, grabar o compartir imágenes, historias clínicas o datos de pacientes por cualquier medio, incluidas redes sociales y mensajería personal.

c) Utilizar los datos únicamente para la finalidad legítima asignada a su rol.

d) Reportar de inmediato cualquier incidente, sospecha de acceso indebido o vulneración de seguridad.

e) Devolver o destruir, a la terminación del vínculo, toda información y credencial de acceso.

f) Asumir las consecuencias laborales, civiles, penales y disciplinarias derivadas del incumplimiento, incluidas las sanciones del artículo 269F del Código Penal colombiano (violación de datos personales).

Artículo 31. Encargados del Tratamiento y Terceros

La Clínica solo transmite datos personales a terceros (laboratorios, centros de imagenología, proveedores tecnológicos, pasarelas de pago, servicios de telemedicina) que hayan celebrado con ella un Acuerdo de Transmisión de Datos / Encargado del Tratamiento (Anexo C), que contempla, como mínimo:

- Identificación de las partes y del tratamiento autorizado.
- Finalidades específicas permitidas, con prohibición expresa de uso secundario.
- Obligación de implementar medidas técnicas y organizativas equivalentes a las de la Clínica.
- Deberes de confidencialidad extendidos a todo el personal del encargado.
- Prohibición de subcontratación sin autorización escrita.
- Auditorías periódicas o presentación de certificaciones (ISO 27001, SOC 2, HIPAA compliance).
- Régimen de responsabilidad, indemnidad y penalidades.
- Obligación de cooperación en la atención de derechos ARCO.
- Devolución o destrucción de datos al término del contrato.

Artículo 32. Laboratorios Dentales y Centros de Imagenología

La relación con laboratorios protésicos, centros de tomografía, servicios de impresión 3D y escaneo intraoral externo exige suscripción de Acuerdos de Encargo reforzados, con cláusulas específicas sobre:

- Transmisión cifrada de archivos DICOM, STL, PLY y metadatos clínicos.
- Uso exclusivo para la finalidad de fabricación del dispositivo o análisis solicitado.
- Prohibición de conservar copias más allá del plazo técnicamente necesario.
- Trazabilidad de entregas y recepciones.

TÍTULO IX — POLÍTICA DE COOKIES

Artículo 33. Uso de Cookies en el Sitio Web

El sitio web www.armoniadentofacial.co utiliza cookies y tecnologías equivalentes (píxeles, identificadores de dispositivo, almacenamiento local) con el propósito de ofrecer una experiencia de navegación segura, funcional y personalizada, medir audiencia y, con consentimiento explícito del visitante, ofrecer contenidos personalizados.

Esta política cumple con los lineamientos de la Directiva ePrivacy (2002/58/CE) y el RGPD para visitantes residentes en la Unión Europea, así como con el California Consumer Privacy Act (CCPA) para residentes de California, EE.UU.

Artículo 34. Tipología de Cookies Utilizadas

Tipo	Finalidad	Base legal
Técnicas / estrictamente necesarias	Funcionamiento del sitio, sesión, seguridad	Interés legítimo (exento de consentimiento)
De preferencias	Idioma, región, configuración de usuario	Consentimiento
Analíticas	Medición de audiencia, estadística anónima	Consentimiento
Publicitarias	Remarketing, perfiles publicitarios	Consentimiento explícito
De terceros	Integración de mapas, videos, redes sociales	Consentimiento explícito

Artículo 35. Gestión del Consentimiento y Preferencias

Al ingresar por primera vez al sitio web, el visitante visualizará un banner de cookies que le permitirá:

16. Aceptar todas las cookies.
17. Rechazar las cookies no esenciales.
18. Configurar granularmente su preferencia por categoría.
19. Acceder en todo momento al panel "Gestionar cookies" ubicado en el pie de página.

El consentimiento otorgado podrá ser revocado en cualquier momento, sin que esto afecte la licitud del tratamiento previo a su retiro. La Clínica conserva el registro de consentimientos durante un periodo no inferior a veinticuatro (24) meses como evidencia de cumplimiento.

TÍTULO X — CONSENTIMIENTO INFORMADO PARA TELEMEDICINA Y CONSULTA VIRTUAL

> **Cláusula indispensable para servicios de teleconsulta**
>
> *La presente cláusula desarrolla el consentimiento informado específico exigido por la Resolución 2654 de 2019 del Ministerio de Salud de Colombia para la prestación de servicios de telesalud y telemedicina. Su aceptación es requisito sine qua non para acceder a la atención virtual y debe firmarse de manera independiente al consentimiento general del tratamiento de datos.*

Artículo 36. Naturaleza y Modalidades del Servicio

La Clínica ofrece, como complemento de su atención presencial, servicios de telemedicina en las siguientes modalidades reconocidas por la normativa colombiana:

a) Telemedicina interactiva (sincrónica): videoconsulta en tiempo real entre paciente y profesional.

b) Telemedicina no interactiva (asincrónica): envío diferido de información, imágenes o documentos para análisis.

c) Tele-experticia: interconsulta entre profesionales.

d) Telemonitoreo: seguimiento remoto de variables clínicas postoperatorias.

Artículo 37. Limitaciones Clínicas y Alcance

El paciente declara comprender y aceptar que:

20. La teleconsulta es una herramienta complementaria, no sustitutiva, de la atención presencial, y sus alcances diagnósticos y terapéuticos están limitados por la ausencia de examen físico directo.
21. El profesional tratante podrá, en cualquier momento, determinar que el caso requiere consulta presencial, procedimiento o derivación urgente, la cual será recomendada al paciente.
22. La teleconsulta no es apta para urgencias médicas u odontológicas; ante síntomas de emergencia (sangrado abundante, dolor intenso, edema severo, signos de infección sistémica), el paciente debe dirigirse al servicio de urgencias más cercano.
23. La calidad de la videoconsulta depende de la conexión a internet del paciente; interrupciones o fallas técnicas podrán requerir reprogramación sin costo adicional.

Artículo 38. Plataformas Tecnológicas y Seguridad

La Clínica utiliza plataformas de videoconferencia clínica que cumplen los siguientes requisitos:

- Cifrado extremo a extremo (E2EE) de la señal de audio y video.
- Certificación HIPAA-compliant y, cuando aplique, cláusula BAA firmada con el proveedor.

- Acceso mediante enlace único, cifrado y de un solo uso, con sala de espera virtual.
- Almacenamiento de credenciales y metadatos en servidores con cifrado en reposo AES-256.
- Autenticación del profesional mediante MFA y verificación de identidad del paciente al inicio de la consulta.

Artículo 39. Grabación, Documentación y Registro Clínico

Respecto al tratamiento audiovisual de la teleconsulta, el paciente queda expresamente informado:

a) Toda teleconsulta genera un registro en la historia clínica electrónica, con hora de inicio y fin, motivo de consulta, hallazgos, plan y recomendaciones.

b) La Clínica podrá, con consentimiento explícito, adicional y específico del paciente, grabar la sesión con fines estrictamente clínicos, docentes o de auditoría de calidad.

c) El paciente queda notificado de la prohibición absoluta de grabar, fotografiar o difundir la consulta sin autorización expresa del profesional tratante, conforme al derecho al buen nombre e imagen.

d) Cualquier grabación se conservará cifrada en los sistemas clínicos, con acceso restringido y por los plazos de conservación de la historia clínica.

Artículo 40. Manifestación de Consentimiento Informado para Telemedicina

> **Declaración del paciente (formato incluido en Anexo D)**
>
> *Yo, [nombre completo], identificado(a) con [documento], actuando en nombre propio o en representación de [paciente], declaro que he sido informado(a) en lenguaje claro y comprensible sobre la naturaleza, alcances, beneficios, limitaciones y riesgos del servicio de telemedicina ofrecido por la Clínica Armonía Dento-Facial. He tenido la oportunidad de formular preguntas y recibir respuestas satisfactorias. Autorizo de manera libre, expresa e informada la realización de la teleconsulta y el tratamiento de mis datos personales y clínicos exclusivamente para las finalidades descritas en la política de privacidad. Reconozco que puedo revocar este consentimiento en cualquier momento y solicitar atención presencial.*

TÍTULO XI — DISPOSICIONES FINALES

Artículo 41. Vigencia, Actualizaciones y Control de Versiones

La presente política entra en vigor desde la fecha de su publicación en el sitio web oficial de la Clínica y permanecerá vigente hasta tanto no sea modificada por una versión posterior. La Clínica se reserva el derecho de actualizarla para adaptarla a cambios normativos, tecnológicos o de negocio; las modificaciones sustanciales serán notificadas a los Titulares por correo electrónico o mediante aviso destacado en el sitio web, con una antelación mínima de diez (10) días hábiles antes de su entrada en vigor.

Artículo 42. Legislación Aplicable y Jurisdicción

La presente política se rige por las leyes de la República de Colombia. Sin perjuicio de lo anterior, para los pacientes sujetos al RGPD o a la HIPAA se aplicarán, adicionalmente, las disposiciones más protectoras derivadas de dichas normativas. Cualquier controversia será resuelta preferentemente por mecanismos alternativos de solución de conflictos y, en subsidio, por los jueces competentes del domicilio de la Clínica.

Artículo 43. Autoridad de Control y Canal de Quejas

El Titular podrá presentar queja o reclamación ante la autoridad competente:

a) Colombia — Superintendencia de Industria y Comercio (SIC): www.sic.gov.co · Carrera 13 No. 27-00, Bogotá · notificacionesjudiciales@sic.gov.co

b) Unión Europea — Autoridad nacional de protección de datos del Estado miembro de residencia (AEPD España, CNIL Francia, BfDI Alemania, etc.).

c) Estados Unidos — Office for Civil Rights (HHS.gov/OCR) para asuntos HIPAA.

ANEXOS — FORMATOS TIPO

Anexo A — Formato de Autorización para el Tratamiento de Datos Personales

Yo, _____, identificado(a) con documento No. _____, en calidad de Titular (o representante legal de _____), actuando libre, expresa e informadamente, AUTORIZO a la Clínica Armonía Dento-Facial, identificada con NIT _____, a recolectar, almacenar, usar, circular, suprimir, transferir y transmitir mis datos personales de identificación, contacto, salud, imágenes diagnósticas y financieros, con las finalidades descritas en la Política de Tratamiento de Datos Personales, que declaro haber leído y comprendido, y que se encuentra publicada en www.armoniadentofacial.co/privacidad.

Marque con una X las finalidades que autoriza:

- [ ] Finalidades administrativas y de gestión de citas.
- [ ] Finalidades asistenciales, clínicas y diagnósticas.
- [ ] Uso de imágenes clínicas con fines de marketing o casos de estudio.
- [ ] Transferencia internacional de mis datos para continuidad asistencial.
- [ ] Envío de boletines, promociones y contenidos educativos.

Firma del Titular o representante legal: _____ Fecha: _____

Anexo B — Acuerdo de Confidencialidad para Personal Interno

Entre la Clínica Armonía Dento-Facial y el (la) colaborador(a) _____, se suscribe el presente Acuerdo de Confidencialidad y Deber de Reserva Clínica, en los siguientes términos:

PRIMERA — Objeto. El (la) colaborador(a) se obliga a guardar reserva absoluta sobre toda información a la que acceda en ejercicio de sus funciones, incluyendo datos personales de pacientes, historias clínicas, imágenes diagnósticas, información financiera, procesos internos y secretos comerciales de la Clínica.

SEGUNDA — Alcance temporal. La obligación de confidencialidad se mantendrá durante la vigencia del contrato laboral o de prestación de servicios y por un plazo de cinco (5) años posteriores a su terminación, sin perjuicio de las obligaciones legales permanentes del secreto profesional.

TERCERA — Prohibiciones. Queda expresamente prohibido: (i) compartir información por cualquier medio; (ii) fotografiar, grabar o copiar registros clínicos; (iii) acceder a información fuera del ámbito de sus funciones; (iv) divulgar credenciales; (v) retirar documentos o dispositivos sin autorización.

CUARTA — Consecuencias del incumplimiento. El incumplimiento será causa justa de terminación del vínculo, sin perjuicio de las acciones penales (Art. 269F C.P.), civiles, disciplinarias y administrativas correspondientes.

Firmas: Colaborador _____ C.C. _____ Clínica (representante legal) _____
Fecha: _____

Anexo C — Acuerdo Marco de Encargo del Tratamiento (Resumen)

Este anexo contiene el modelo de acuerdo que la Clínica suscribirá con todo encargado del tratamiento (laboratorios, centros de imagenología, proveedores de software clínico, pasarelas de pago, plataformas de telemedicina, servicios en la nube). El texto completo se adjunta al contrato marco respectivo.

- Objeto y descripción del tratamiento delegado.
- Categorías de datos e interesados.
- Duración y finalidades específicas.
- Obligaciones técnicas y organizativas mínimas (cifrado, MFA, auditoría).
- Régimen de subcontratación (prohibición sin autorización escrita).
- Cooperación ante derechos ARCO y ante incidentes.
- Devolución / destrucción certificada al término.
- Responsabilidad y penalidades.
- Cláusulas contractuales tipo para transferencia internacional.

Anexo D — Consentimiento Informado para Telemedicina

Formato completo, firmable electrónica o presencialmente, que reproduce la manifestación del Artículo 40 con espacios para datos del paciente, fecha, firma y aceptación expresa de cada uno de los numerales del Título X.

Anexo E — Formato de Solicitud de Derechos ARCO

Nombre completo: _____ Documento: _____

Correo / dirección para notificaciones: _____

Derecho que ejerce (marque): [ ] Acceso [ ] Rectificación [ ] Cancelación [ ] Oposición [ ] Portabilidad [ ] Olvido [ ] Limitación

Descripción clara de la solicitud: _____

Documentos que anexa: _____

Firma: _____ Fecha: _____

IDENTIFICACIÓN DOCUMENTAL

Documento: Sistema Integral de Protección de Datos Personales, Política de Privacidad y Acuerdos de Confidencialidad.

Responsable: Clínica Armonía Dento-Facial — Oficial de Protección de Datos (DPO).

Versión: 1.0 · Fecha de expedición: abril de 2026.

Próxima revisión programada: abril de 2027 o antes ante cambios normativos sustantivos.

Canal de contacto: protecciondedatos@armoniadentofacial.co | dpo@armoniadentofacial.co